REMARKS/ARGUMENTS

In view of the foregoing amendments and the following remarks, reconsideration of this application is requested. Claims 1-22 are now pending with claims 1, 9, and 12 being independent. Claims 1-12 have been amended. Claim 23 has been cancelled. No new matter has been added.

Amended claim 1 describes an electronic device including an authorization control circuit, comprising: a data storage including one or more data files, wherein each of the data files is a digital audio file, video file, or multimedia file; a digital signal processor operably coupled to the data storage, said digital signal processor operable to provide digital data output, determine an authorization state by receiving a data file selected by a user from the one or more data files, hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy, and generating a disable signal, wherein the disable signal is also capable of being generated when the electronic device satisfies one or more sleep conditions; a digital to analog converter operably coupled to the digital signal processor and operable to receive the digital data output, convert the digital data to corresponding analog data, output the corresponding analog data, and mute the output of the corresponding analog data; and the digital to analog converter including an input operable to receive the disable signal, and the digital to analog converter muting the output of the corresponding analog data without adding noise artifacts in response to the disable signal.

Amended claim 9 describes an electronic device including an authorization control circuit, comprising: a data storage including one or more data files, wherein each of the data files is a digital audio file, video file, or multimedia file; a digital signal processor operably coupled to the data storage, said digital signal processor operable to provide digital data output, determine an authorization state by receiving a data file selected by a user from the one or more data files, hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy, and generating a disable signal, wherein the disable signal is also capable of being generated when the electronic device satisfies one or more sleep conditions; a digital to analog converter operably coupled to

the digital signal processor and operable to receive the digital data output, convert the digital data to corresponding analog data, and output the corresponding analog data; and an analog amplifier operable to receive the analog output from the digital to analog converter and generate amplified output, and having an input operable to receive the disable signal, the amplifier muting the amplified output without adding noise artifacts in response to the disable signal.

Amended claim 12 describes a method of selectively muting output in an electronic device. The method includes the steps of: generating digital data; determining an authorization state, wherein determining the authorization state comprises: selecting a data file from one or more data files in a data storage device, wherein the data file is a digital audio file, video file, or multimedia file, said data file including the digital data; performing a hashing function on the data file to generate a fixed-length value or key representing the data file, wherein the hashing function is executed by a digital signal processor; comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or is an invalid copy; generating a disable signal, wherein the disable signal is also capable of being generated when the electronic device satisfies one or more sleep conditions; transmitting the digital data to a digital to analog converter; generating an analog signal corresponding to the digital data; transmitting the disable signal to the digital to analog converter; and muting the analog signal without adding noise artificats in response to the transmitted disable signal.

Claims 1-18 and 21-22 stand rejected under 35 U.S.C. § 103(a) as obvious over DeLuca et al. (5,612,682) in view of Seo et al. (5,063,597) and further in view of Tran (5,734,729) and even further in view of Nagata (6,114,981). Applicant requests reconsideration and withdrawal of these rejections for at least the reason that DeLuca, Seo, Tran, and Nagata do not describe or suggest a data storage including one or more **data files**, wherein each of the data files is a **digital audio file, video file,** or **multimedia file**; a digital signal processor operably coupled to the data storage, said digital signal processor operable to provide digital data output, determine an authorization state by receiving a data file selected by a user from the one or more data files, **hashing the data file** to generate a **fixed-length value** or **key** representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**, and generating a disable signal. Furthermore, DeLuca, Seo, Tran and Nagata do not describe or

suggest muting the output of the corresponding analog data **without adding noise artifacts** in response to the disable signal.

DeLuca, in the Abstract, teaches a method and apparatus in a communication system operated by a service provider that controls utilization of a module added to a portable communication device including a transceiver which communicates with a fixed portion of the communication system. The portable communication device receives a request for utilization of the module. In response, the portable communication device acts to obtain a usage authorization for utilizing the module. The portable communication device disallows the utilization of the module, in response to the usage authorization being unobtainable. No part of the DeLuca reference describes or suggests how to determine an authorization state by **hashing the data file** to generate a **fixed-length value** or **key** representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**. Furthermore, the Examiner on page 7 of the Office Action mailed March 28, 2008 admits "DeLuca ... fails to teach performing a hash function on the data file by the DSP."

Seo fails to remedy the failure of DeLuca to describe or suggest how to determine an authorization state by **hashing the data file** to generate a **fixed-length value** or **key** representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**. Seo, in the Abstract and Figure 3, teaches a muting circuit in a digital audio system having a digital signal processor, a first latch, a second latch, a comparator for comparing data in the first and second latches, an address encoder, a counter, a memory, a divider, a multiplier and a switching circuit. Disturbing beat noises generated during the turning off of power to the system or null data pop noises generated in response to external influences or internal circuitry influences are muted. Seo does not describe or suggest how to determine an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy.

Tran fails to remedy the failure of DeLuca and Seo to describe or suggest how to determine an authorization state by **hashing the data file** to generate a **fixed-length value** or

key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**. Tran, at column 2, lines 31-42, describes an audio power management system that eliminates audible noise associated with waking up or putting a computer to sleep, using a speaker mute signal. Tran does not describe or suggest how to determine an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy.

Nagata fails to remedy the failure of DeLuca, Seo, and Tran to describe or suggest how to determine an authorization state by **hashing the data file** to generate a **fixed-length value** or **key** representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**.. Nagata, in the Abstract, teaches an over-sampling D/A converter that has a mute function for fixing an average DC potential of an analog output signal to a predetermined potential, and comprises a sigma delta modulator for receiving a multibit digital signal to which a DC offset value is added and then outputting a one-bit non-return-to-zero signal. Nagata does not describe or suggest how to determine an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy. For at least these reasons, Applicant respectfully submits that claims 1, 9, and 12 are patentable over DeLuca in view of Seo and further in view of Tran and even further in view of Nagata.

Claims 2-8 and 21-22 depend from independent claim 1, claims 10-11 depend from independent claim 9, and claims 13-18 depend from independent claim 12. Accordingly, Applicant requests reconsideration and withdrawal of the rejections for claims 2-8, 10-11, 13-18, and 21-22 for the reasons discussed above with respect to claims 1, 9 and 12.

Claims 19-20 stand rejected under 35 U.S.C. § 103(a) as obvious over DeLuca et al. (5,612,682) in view of Seo et al. (5,063,597) and further in view of Tran (5,734,729) and even further in view of Nagata (6,114,981) and still further in view of Lipovski (6,675,002). Applicant requests reconsideration and withdrawal of these rejections for at least the reason that DeLuca,

Seo, Tran, Nagata and Lipovski do not describe or suggest how to determine an authorization state by **hashing the data file** to generate a **fixed-length value** or **key** representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**.

No part of the DeLuca, Seo, Tran or Nagata references, as mentioned above, describes or suggests how to determine an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy. Lipovski fails to remedy the failure of DeLuca, Seo, Tran, and Nagata to describe or suggest how to determine an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy. Lipovski makes no mention of determining an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the data file has been changed or an invalid copy. For at least these reasons, Applicant respectfully submits that claims 19-20 are patentable over DeLuca in view of Seo and further in view of Tran (5,734,729) and even further in view of Nagata (6,114,981) and still further in view of Lipovski.

Canceled claim 23 was rejected under 35 U.S.C. § 103(a) as obvious over DeLuca et al. (5,612,682) in view of Seo et al. (5,063,597) and further in view of Tran (5,734,729) and even further in view of Nagata (6,114,981) and still further in view of Fette et al. (6,052,600). Applicant states that DeLuca, Seo, Tran, Nagata and Fette do not describe or suggest how to determine an authorization state by hashing the **data file** to generate a **fixed-length value** or **key** representing the **data file**, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the **data file has been changed or an invalid copy**.

No part of the DeLuca, Seo, Tran or Nagata references, as mentioned above, describes or suggests how to determine an authorization state by hashing the data file to generate a fixed-length value or key representing the data file, comparing the fixed-length value or key to an expected fixed-length value or key for the data file, wherein the comparison determines if the

data file has been changed or an invalid copy. Fette fails to remedy the failure of DeLuca, Seo, Tran, and Nagata to describe or suggest how to determine an authorization state by hashing the **data file** to generate a **fixed-length value** or **key** representing the **data file**, comparing the fixed-length value or key to an expected fixed-length value or key for the **data file**, wherein the comparison determines if the **data file** has been changed or is an invalid copy. The Examiner on page 7 of the Office Action cites to Fette, column 9 lines 5-15 "hash of the software program to compare to a predetermined basis." Fette in Figures 3 and 4 and columns 8-9 describes hash of a software program and not a data file including digital data that is a digital audio file, video file or multimedia file. For at least these reasons, Applicant respectfully submits that claims 1-22 are patentable over DeLuca in view of Seo and further in view of Tran (5,734,729) and even further in view of Nagata (6,114,981) and still further in view of Fette.

Examiner Nalven is requested to contact Applicants' representative Indranil Chowdhury at (281) 772-9361 for further clarification and amendments to the claims for prompt prosecution and allowance of this application.

In view of these remarks and amendments, Applicant submits that this application is now in condition for allowance and the Examiner's prompt action in accordance therewith is respectfully requested. To the extent necessary, the Applicants petition for an Extension of Time under 37 CFR 1.136. The Commissioner is authorized to charge any additional fees, including extension of time fees, and/or credit any overpayment to Deposit Account 20-0668 of Texas Instruments Incorporated.

Respectfully submitted,

/Indranil Chowdhury/

Indranil Chowdhury
Reg. No. 47,490
Attorneys for Applicant

Robert D. Marshall, Jr.
Texas Instruments Incorporated
P.O. Box 655474, MS 3999
Dallas, TX 75265
(972) 917-5290